

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Motokazu KAWAKI

GAU:

SERIAL NO: NEW APPLICATION

EXAMINER:

FILED: HERewith

FOR: CONTENTS REPRODUCING APPARATUS, CONTENTS REPRODUCTION CONTROL PROGRAM
AND RECORDING MEDIUM HAVING A CONTENTS REPRODUCTION CONTROL PROGRAM
RECORDED THEREON

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

- ☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of 35 U.S.C. §120.
- ☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of 35 U.S.C. §119(e): Application No. Date Filed
- ☒ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of 35 U.S.C. §119, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

<u>COUNTRY</u>	<u>APPLICATION NUMBER</u>	<u>MONTH/DAY/YEAR</u>
Japan	2002-333546	November 18, 2002

Certified copies of the corresponding Convention Application(s)

- ☒ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee
- ☐ were filed in prior application Serial No. filed
- ☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.
- ☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and
- ☐ (B) Application Serial No.(s)
☐ are submitted herewith
☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Marvin J. Spivak

Registration No. 24,913

Customer Number

22850

Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

C. Irvin McClelland
Registration Number 21,124

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application:

2002年11月18日

出 願 番 号
Application Number:

特願2002-333546

[ST.10/C]:

[JP2002-333546]

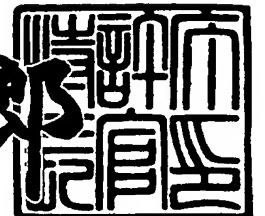
出 願 人
Applicant(s):

三菱電機株式会社

2003年 6月13日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3046435

【書類名】 特許願

【整理番号】 543128JP01

【提出日】 平成14年11月18日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 17/60
G06F 13/00

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社
社内

【氏名】 河木 理一

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100102439

【弁理士】

【氏名又は名称】 宮田 金雄

【選任した代理人】

【識別番号】 100092462

【弁理士】

【氏名又は名称】 高瀬 彌平

【手数料の表示】

【予納台帳番号】 011394

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記録した記録媒体

【特許請求の範囲】

【請求項 1】 暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えたことを特徴とするコンテンツ再生装置。

【請求項 2】 前記コンテンツ再生制御手段により起動され、前記コンテンツデータの利用制限情報に従って入力手段から入力される操作信号を無効にする利用制限制御手段を設けたことを特徴とする請求項 1 に記載のコンテンツ再生装置。

【請求項 3】 ネットワークに接続するインターフェース部が設けられ、前記ネットワークに接続したサーバ装置から前記暗号化データを取得するようにしたことを特徴とする請求項 1 に記載のコンテンツ再生装置。

【請求項 4】 媒体読取手段が設けられ、この媒体読取手段により記録媒体に記録された前記暗号化データを取得するようにしたことを特徴とする請求項 1 に記載のコンテンツ再生装置。

【請求項 5】 保存手段に保存された暗号化データを取得し、この暗号化データから復元したコンテンツデータにより再生したイメージデータをブラウザのブラウザ画面上に表示させるコンピュータに、入力手段から入力された識別情報に基づき前記ブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ

及びその利用制限情報を一時的に記憶手段に記憶する記憶処理と、前記コンテンツデータの利用制限情報に応じて前記ブラウザ画面上にブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とを実現させることを特徴とするコンテンツ再生制御プログラム。

【請求項 6】 保存手段に保存された暗号化データを取得する処理と、入力手段から入力された識別情報と予め記憶した識別情報とを照合して前記識別情報を入力した利用者の使用許可又は不許可を判別する認証処理と、前記認証処理の判別結果に基づいてブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を記憶手段に一時的に記憶する記憶処理と、前記記憶手段に記憶した前記コンテンツデータによりイメージデータを再生して前記ブラウザ画面上に表示させる表示処理と、前記コンテンツデータの利用制限情報に応じてブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とをコンピュータに実現させることを特徴とするコンテンツ再生制御プログラム。

【請求項 7】 前記識別情報は、ユーザ ID とパスワードであることを特徴とする請求項 5 又は請求項 6 に記載のコンテンツ再生制御プログラム。

【請求項 8】 前記利用制限情報は、利用者毎に登録された複数の利用制限情報であることを特徴とする請求項 5 又は請求項 6 に記載のコンテンツ再生制御プログラム。

【請求項 9】 請求項 5 又は請求項 6 に記載のコンテンツ再生制御プログラムを記録したことを特徴とするプログラム記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、インターネット、イントラネット等の電気通信回線、CD-ROM等の記憶媒体により配布されるデジタルコンテンツ（文字、画像あるいは動画等）をブラウザのブラウザ画面上に表示して閲覧する際に、このブラウザ画面上

に表示されたこれらデジタルコンテンツの印刷、保存等の利用を制限し、利用者による不正利用ないし第三者への情報漏洩を防止するコンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記憶した記録媒体に関する。

【0002】

【従来の技術】

近年、インターネットの利用者が急増し、インターネットは情報流通あるいはサービス提供のインフラとして不可欠な存在となりつつある。例えば、これまではCD-ROM、書籍等の有体物として流通していたコンピュータプログラムや書籍等のいわゆる情報財はパソコンや携帯電話等をつなぐネットワーク上で流通するようになっており、さらにオンラインゲームや電子掲示板の提供等の各種サービスも生まれている。

【0003】

一方、このようなインターネットの普及に伴い、ネットワークの中を流通する情報の改ざんや不正利用等が行われる危険性も同時に増加しており、今後、プログラム、画像コンテンツ等の流通を普及・促進するためにはこのようなネットワーク内を流通し、パソコン等において表示される情報の不正利用や改ざんを防止するための対策が不可欠となっている。

【0004】

例えば、このような不正利用を防止する技術として、Digital Rights Management（以下、単にDRMという。）と呼ばれる技術がある。このDRM技術は、どういう利用ができるかの著作権情報とコンテンツとを暗号化して送信し、条件に合致した利用者のみが当該暗号を解読してコンテンツの内容を視聴できるようにするという技術であり、暗号化された条件の設定により、コンテンツを再生できる回数、コンテンツを視聴できる期間、CDやDVDへの保存の可否等を任意に設定することが可能である。

【0005】

なお、パソコン等の端末装置において受信された画像コンテンツ、例えばWebページ等はブラウザを用いて表示させるのが一般的である。このWebブラウザ

は、Uniform Resource Locator（以下、URLという。）によって指定されたWebコンテンツの要求とこれらの表示を実行するためのアプリケーション・プログラムであり、ハイパーテキスト転送プロトコル（以下、HTMLという）の要求の中でURLを指定する。この要求はURLによって指定された情報やコンテンツをサポートするWebサーバ装置に転送され、対応するコンテンツがWebサーバ装置から要求のあった端末装置に対して送信される。

【0006】

【特許文献1】

特開2002-229447公報（第4頁左欄第29行目乃至同頁右欄第5行目の記載事項を参照。）

【0007】

【発明が解決しようとする課題】

しかしながら、従来のWebブラウザ等のアプリケーション・プログラムは、文字、画像コンテンツ等の公開を念頭に設計されているため、パソコン等のブラウザ画面上に表示された後のコンテンツはブラウザの印刷機能やファイル保存機能等によってWebサイト利用者の手元に簡単に保存することができるよう構成されており、たとえ暗号化されたデジタルコンテンツを配信するように構成されていても、暗号化データを復号化するのみで表示後のデジタルコンテンツの利用を制限する配慮が何らなされていない場合には、これら表示後のデジタルコンテンツが利用者により不正に利用され、容易に漏洩してしまうという問題点があった。

【0008】

これに対し、閲覧のみを許可して印刷やファイル保存等は許可しないようにするという機能をブラウザの機能として付加することも可能であるが、そのためにはそのような機能を有する新規なWebブラウザを作成しなければならず、また、一般に公開されているWebブラウザを利用する場合には無断でそのような機能を設けることはできない等の問題点があった。

【0009】

また、DRM技術を使用する場合には、コンテンツの配信を行うサーバ装置とは別に著作権情報管理サーバと呼ばれる専用のサーバ装置を設ける必要があり、課金に応じたコンテンツの視聴等、様々なビジネスモデルに対応する条件設定が可能となる一方、このような特別のサーバ装置を設置しなければならないというシステム上の問題点がある。

【0010】

この発明は上記のような課題を解消するためになされたもので、特別のサーバ装置等を設けることなく、また、一般に公開されているブラウザを利用したまま当該ブラウザ画面上に表示されたデジタルコンテンツの不正利用ないし第三者への漏洩を防止することができる新規なコンテンツ再生装置、コンテンツ再生制御プログラム及びコンテンツ再生制御プログラムを記録した記録媒体を提供することを目的とする。

【0011】

【課題を解決するための手段】

請求項1の発明に係るコンテンツ再生装置は、暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えたものである。

【0012】

請求項2の発明に係るコンテンツ再生装置は、前記コンテンツ再生制御手段により起動され、前記コンテンツデータの利用制限情報に従って入力手段から入力される操作信号を無効にする利用制限制御手段を設けたものである。

【0013】

請求項 3 の発明に係るコンテンツ再生装置は、ネットワークに接続するインターフェース部が設けられ、前記ネットワークに接続したサーバ装置から前記暗号化データを取得するようにしたものである。

【 0 0 1 4 】

請求項 4 の発明に係るコンテンツ再生装置は、媒体読取手段が設けられ、この媒体読取手段により記録媒体に記録された前記暗号化データを取得するようにしたものである。

【 0 0 1 5 】

請求項 5 の発明に係るコンテンツ再生制御プログラムは、保存手段に保存された暗号化データを取得し、この暗号化データから復元したコンテンツデータにより再生したイメージデータをブラウザのブラウザ画面上に表示させるコンピュータに、入力手段から入力された識別情報に基づき前記ブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶手段に記憶する記憶処理と、前記コンテンツデータの利用制限情報に応じて前記ブラウザ画面上にブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブラウザ補助機能処理とを実現させるものである。

【 0 0 1 6 】

請求項 6 の発明に係るコンテンツ再生制御プログラムは、保存手段に保存された暗号化データを取得する処理と、入力手段から入力された識別情報と予め記憶した識別情報とを照合して前記識別情報を入力した利用者の使用許可又は不許可を判別する認証処理と、前記認証処理の判別結果に基づいてブラウザ画面上に生成されるコンテンツ利用機能を使用禁止にする禁止処理と、前記暗号化データの復号化処理により復元されたコンテンツデータ及びその利用制限情報を記憶手段に一時的に記憶する記憶処理と、前記記憶手段に記憶した前記コンテンツデータによりイメージデータを再生して前記ブラウザ画面上に表示させる表示処理と、前記コンテンツデータの利用制限情報に応じてブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するブ

ブラウザ補助機能処理とをコンピュータに実現させるものである。

【0017】

請求項7の発明に係るコンテンツ再生制御プログラムは、前記識別情報がユーザIDとパスワードであるものである。

【0018】

請求項6の発明に係るコンテンツ再生制御プログラムは、利用者毎に登録された複数の利用制限情報であるものである。

【0019】

請求項9の発明に係るプログラム記録媒体は、請求項5又は請求項6に記載のコンテンツ再生制御プログラムを記録したことを特徴とするものである。

【0020】

【発明の実施の形態】

実施の形態1.

以下、この発明の実施の形態1について図1乃至図6を用いて説明する。図1は実施の形態1によるコンテンツ再生方法を実現するためのシステム構成図、図2はコンテンツ再生装置等の具体的構成を示す機能ブロック図である。図1及び図2において、1はWebコンテンツのコンテンツデータを保存するWebサーバー装置（以下、サーバ装置という。）、2はインターネット、イントラネット等の電気通信回線（以下、ネットワークという。）、3はネットワーク2を介してサーバ装置1と接続したパソコン、携帯情報端末（PDA）等であって、表示部8に生成されたブラウザ画面上にコンテンツデータにより再生したイメージデータ、すなわちWebコンテンツを表示するコンテンツ再生装置である。

【0021】

サーバ装置1には所定の暗号方式を用いて暗号化されたWebコンテンツのコンテンツデータ及びその利用制限情報が保存されており（以下、暗号化データという。）、実施の形態1によるコンテンツ再生装置（以下、端末装置という。）3により閲覧する各Webコンテンツはサーバ装置1からネットワーク2を介して端末装置3に配信（ダウンロード）される。Webコンテンツの種類としては、いわゆるHTMLファイル、各種画像ファイル（BMP形式、GIF形式、J

P E G 形式、P N G 形式等)、P D F ファイル等があり、各コンテンツ毎に対応する利用制限情報が付加されている。

【 0 0 2 2 】

また、端末装置 3 にはサーバ装置 1 からダウンロードした暗号化データを格納する暗号化データ格納部 4、利用制限制御プログラムを格納する利用制限制御ライブラリ格納部 5、コンテンツ再生制御プログラムを格納するコンテンツ再生制御プログラム格納部 6、W e b ブラウザプログラムを格納する W e b ブラウザ格納部 7、及び復号化処理により復元されたコンテンツデータにより再生された W e b コンテンツを表示するブラウザ画面が生成される表示部がそれぞれ設けられており、サーバ装置 1 から配信された暗号化データは端末装置 3 に設けられたネットワーク 2 とのインタフェース部（図示省略する。）を介して暗号化データ格納部 4 に格納される。

【 0 0 2 3 】

なお、実施の形態 1 によるコンテンツ再生装置においては、コンテンツ再生制御プログラムもサーバ装置 1 に保存されており、端末装置 3 の転送要求に応じてサーバ装置 1 からネットワーク 2 を介して端末装置 3 に配信される。端末装置 3 に配信されたコンテンツ再生制御プログラムはインタフェース部を介してコンテンツ再生制御プログラム格納部 6 に格納される。

【 0 0 2 4 】

ここで、暗号化データ格納部 4、利用制限制御ライブラリ格納部 5、及び W e b ブラウザ格納部 7 は、端末装置 3 内のハードディスク等の物理的記憶媒体上にそれぞれ設けているが、コンテンツ再生制御プログラム格納部 6 は、端末装置 3 内のデータを一時的に記憶する電子部品、例えば、R A M (R a n d o m A c c e s s M e m o r y) 等のメモリ上に設けている。すなわち、この発明に係るコンテンツ再生制御プログラムは、R A M 等のメモリ内に格納され、このようなメモリ上で動的に生成させるものである。

【 0 0 2 5 】

また、図 2 において、9、10 はそれぞれサーバ装置 1 内に保存され端末装置 3 にダウンロードされるコンテンツ再生制御プログラム及び暗号化データ、11

はサーバ装置 1 からコンテンツ再生制御プログラム 9 をダウンロードするために起動される呼び出し用 HTML 部である。この呼び出し用 HTML 部 1 1 は、Web ブラウザ格納部 7 に格納された Web ブラウザが起動して表示部 8 にブラウザ画面が生成されるとそのブラウザ画面上に表示される。端末装置 3 の利用者はブラウザ画面上に表示された呼び出し用 HTML 部 1 1 にアクセスすることによりサーバ装置 1 に対するコンテンツ再生制御プログラム 9 の転送要求を行うことができる。

【 0 0 2 6 】

また、1 2 は Web ブラウザ格納部 7 において起動され、HTML で記述された一般の Web コンテンツの解読・表示等を行う Web ブラウザプログラム（以下、Web ブラウザという。）、1 3、1 4 はコンテンツ再生制御プログラム格納部 6 において起動されるコンテンツ再生制御プログラム 9 を構成するライブラリ制御部及び認証部であり、ライブラリ制御部 1 3 は認証部 1 4 及び利用制限制御ライブラリ格納部 5 において起動する利用制限制御ライブラリを構成するキー制御ライブラリ 1 5 の起動を制御する。また、認証部 1 4 は表示部 8 のブラウザ画面上に識別情報、例えば、ユーザ ID とパスワードの入力を促す認証画面を生成して端末装置 3 の利用者に識別情報の入力を求める処理を行う。認証画面内に入力された識別情報と予め記憶した識別情報とが一致すれば、キー制御ライブラリ 1 5 にその旨の認証情報を通知する一方、その識別情報を入力した利用者に対してコンテンツ再生制御プログラム 9 の利用が可能であることを知らせるメッセージをブラウザ画面上に表示する。

【 0 0 2 7 】

また、1 5、1 6 及び 1 7 は利用制限制御ライブラリ格納部 5 において起動される利用制限制御ライブラリを構成するキー制御ライブラリ、インスタンス管理ライブラリ及び復号化ライブラリであり、キー制御ライブラリ 1 5 は認証部 1 4 からの認証情報、及び復号化処理により復元されたコンテンツデータの利用制限情報に基づきブラウザ 1 2 のコンテンツ利用機能の利用制限処理を実行する。インスタンス管理ライブラリ 1 6 はキー制御ライブラリ 1 5 からの指示により起動され、ブラウザ 1 2 の起動状態を確認し、復号化ライブラリ 1 7 は暗号化データ

格納部 4 に格納された暗号化データ 1 0 を復号化処理して元のコンテンツデータ及びその利用制限情報を復元する。

【 0 0 2 8 】

また、1 8 は復号化ライブラリ 1 7 の復号化処理により復元されコンテンツ再生制御プログラム格納部 6 に一時的に記憶された平文のコンテンツデータ（以下、平文コンテンツという。）、1 9 は同様に復号化ライブラリ 1 7 の復号化処理により復元されコンテンツ再生制御プログラム格納部 6 に一時的に記憶された平文コンテンツ 1 8 の利用制限情報、2 0 はコンテンツ再生制御プログラム 9 の制御により利用不可となったブラウザ 1 2 のコンテンツ利用機能に相当するブラウザ補助機能を表示部 8 のブラウザ画面上に生成し、利用制限情報 1 9 に従って当該機能の操作を利用者に促すブラウザ補助機能プログラム（以下、ブラウザ補助機能という。）、2 1 は平文コンテンツ 1 8 からイメージデータを再生して表示部 8 のブラウザ画面上に表示する処理を行う表示処理部である。

【 0 0 2 9 】

なお、図 3 は端末装置 3 に配信される暗号化データ 1 0 のデータ構成を示すデータ構成図である。図 3 において平文コンテンツ 1 8 及びその利用制限情報 1 9 は所定の暗号方式によって暗号化された状態を示しており、図 3 に示すように、暗号化データ 1 0 は所定の暗号方式によって暗号化された平文コンテンツ 1 8 及び利用制限情報 1 9 を一体化することにより生成している。そして、このような使用制限情報 1 9 が平文コンテンツ 1 8 と併せて復元されることにより利用者による不正利用、第三者への情報の漏洩を防止している。この平文コンテンツ 1 8 及び利用制限情報 1 9 には異なる暗号方式を使用することができる。例えば、平文コンテンツ 1 8 は鍵 A、利用制限情報 1 9 は別の鍵 B を用いて暗号化することができ、異なる暗号方式を使用することにより端末装置 3 に配信されるまでのネットワーク 2 内における情報の漏洩、改ざん等を確実に防止することができる。

【 0 0 3 0 】

また、図 3 に示すように、利用制限情報 1 9 は利用者毎に登録することができる。例えば、利用者 A には平文コンテンツ 1 8 に基づきブラウザ画面上に表示さ

れたWebコンテンツの印刷のみを許可する利用制限情報A、利用者Bには平文コンテンツ18に基づきブラウザ画面上に表示されたWebコンテンツの印刷及びファイル保存を許可する利用制限情報B等を登録することができる。このように、一つの平文コンテンツ18に対して複数の利用制限情報(A, B, C, …)を登録することができるので、共通の暗号化データ10を多数の利用者によって利用することができる。

【0031】

次に、動作について図4及び図5を用いて説明する。図4は図1に示す端末装置3の一連の処理について説明するためのフローチャート図、図5は端末装置3の利用制限処理について説明するためのフローチャート図である。端末装置3の利用者がサーバ装置1に保存された暗号化データ10を取得してその中のWebコンテンツの閲覧を行う場合、利用者はまずマウス、キーボード等の入力手段を介して所定のブラウザ12を起動する(S01)。

【0032】

ブラウザ12が起動すると、表示部8にブラウザ12のブラウザ画面が生成され、そのブラウザ画面上に呼び出し用HTML部11が生成される。利用者は呼び出し用HTML部11に表示された呼び出し用HTMLにアクセスすることによりサーバ装置1に対するコンテンツ再生制御プログラム9の転送要求を行う(S02)。サーバ装置1は呼び出し用HTML部11によるコンテンツ再生制御プログラム9の転送要求が行われると、この転送要求を行った端末装置、ここでは端末装置3に対してコンテンツ再生制御プログラム9を配信(ダウンロード)する。コンテンツ再生制御プログラム9はネットワーク2介してダウンロードされ端末装置3に設けられたインタフェース部を介してコンテンツ再生制御プログラム格納部6内に格納される(S02)。

【0033】

サーバ装置1からダウンロードされたコンテンツ再生制御プログラム9がコンテンツ再生制御プログラム格納部6内に格納されると、コンテンツ再生制御プログラム9は起動してコンテンツ再生制御処理を開始する(S03)。

【0034】

コンテンツ再生制御プログラム 9 が起動すると、サーバ装置 1 に保存された暗号化データ 10 がネットワーク 2 を介してダウンロードされ、端末装置 3 内の暗号化データ格納先 4 に保存される (S04)。

【0035】

暗号化データ格納先 4 に暗号化データ 10 が保存されると、コンテンツ再生制御プログラム 9 のライブラリ制御部 13 が起動して認証部 14 による認証処理を起動させる (S05)。

【0036】

認証部 14 は、認証用のダイアログボックス、すなわちユーザ ID、パスワード等の識別情報 (以下、識別情報という。) を入力するための認証画面をブラウザ 12 のブラウザ画面上に生成させ利用者に識別情報の入力を促す。利用者が入力した識別情報と予め記憶した識別情報とが一致しない場合は、暗号化データ格納先 4 に保存されている暗号化データ 10 がその利用者によって閲覧できる暗号化データではないと判断しその後の処理を行わずに処理を終了する。一方、利用者が入力したユーザ ID、パスワードと予め記憶した識別情報とが一致した場合は、認証成功と判断する (S06)。

【0037】

認証部 14 により利用者が入力した識別情報と予め記憶した識別情報とが一致すると判断されると、ライブラリ制御部 13 が利用制限制御ライブラリ格納部 5 内のキー制御ライブラリ 15 を起動して、ブラウザ機能制限処理を実行する一方、認証部 14 の認証情報がキー制御ライブラリ 15 に通知される (S07)。

【0038】

キー制御ライブラリ 15 は、ブラウザ 12 の種類及びバージョンがコンテンツ再生制御プログラム 9 が許可しているか否かを判別し、許可されていないブラウザであると認識した場合はその後の処理を行わずに終了する処理を行う (S08)。判別の結果、許可されているブラウザであると認識した場合はインスタンス管理ライブラリ 16 を起動してブラウザ 12 の起動が継続しているか否かの監視処理を実行する (S09)。

【0039】

また、キー制御ライブラリ 1 5 は、ブラウザ機能制限処理が継続している間、機能制御ライブラリ格納部 5 内の復号化ライブラリ 1 7 を起動して暗号化データ格納部 4 内に保存された暗号化データ 1 0 の復号化処理を実行する。この復号化ライブラリ 1 7 による復号化処理により暗号化データ格納部 4 内に保存された暗号化データ 1 0 から平文コンテンツ 1 8 及び対応する利用制限情報 1 9 がそれぞれ復元される。ここで、暗号化データ 1 0 は利用者毎に設定した複数の利用制限情報を含んでおり、認証部 1 4 において認証成功と判断された識別情報と一致する識別情報を有する利用制限情報、例えば利用者 A であれば利用制限情報 A が復号化ライブラリ 1 7 により復元される。この復元された平文コンテンツ 1 8 及び利用制限情報 A はコンテンツ再生制御プログラム格納部 6 内に保存される（S 1 0）。

【 0 0 4 0 】

キー制御ライブラリ 1 5 は、復元された利用制限情報 A から当該利用者に対して許可されたブラウザ 1 2 のコンテンツ利用機能の有無を判断し（S 1 1）、許可された機能があればその機能の実行にあたるキー入力の監視を解除する処理を行う（S 1 2）。一方、コンテンツ再生制御プログラム 1 0 は、利用制限情報 1 9 に登録された利用制限規則から当該利用者に対して許可されたコンテンツ利用機能の有無を判断し、許可された機能があればブラウザ補助機能 2 0 として表示部 8 のブラウザ画面上に生成する（S 1 3）。各利用者はブラウザ画面上に表示されたブラウザ補助機能 2 0 を利用することによりブラウザ画面上に表示された Web コンテンツを利用することができ、このブラウザ補助機能 2 0 を利用してブラウザ画面上に表示された Web コンテンツの印刷、保存等を行う。

【 0 0 4 1 】

このように、復号化ライブラリ 1 7 の復号化処理によって暗号化データ 1 0 から平文コンテンツ 1 8 及び利用者の識別情報に一致する利用制限情報、例えば利用制限情報 A がそれぞれ復元され（S 1 4）、復元された平文コンテンツ 1 8 については表示処理部 2 1 がその平文コンテンツ 1 8 に基づきイメージデータ、すなわち Web コンテンツを再生し表示部 8 のブラウザ画面上に表示する（S 1 5）。

【 0 0 4 2 】

この際、平文コンテンツ 1 8 及び利用制限情報 1 9 はすべてコンテンツ再生制御プログラム格納部 6、すなわち端末装置 3 内に設けられた R A M 等のメモリ上のみで管理されるので、これら平文コンテンツ 1 8 及び利用制限情報 1 9 が端末装置 3 内のハードディスクやキャッシュ等に残らず、情報の漏洩を防止することができ、ブラウザ画面上に表示されたコンテンツの安全性が保証される。

【 0 0 4 3 】

このように、サーバ装置 1 からダウンロードされる暗号化データ 1 0 には、W e b コンテンツを再生するための平文コンテンツ 1 8 とこの平文コンテンツ 1 8 に再生された W e b コンテンツを閲覧する際の利用制限規則を記述した利用制限情報 1 9 とが含まれているので、各利用者は、識別情報（ユーザ I D とパスワード等）の一致する利用制限情報 1 9 に記述された利用制限規則に従って平文コンテンツ 1 8 の利用を行うことができる。すなわち、W e b コンテンツの配信側は各利用者に応じた複数の利用制限情報 1 9 と平文コンテンツ 1 8 とからなる暗号化データ 1 0 をサーバ装置 1 に保存しておき、各利用者は自分の識別情報に一致する利用制限情報 1 9 に記述された利用制限規則に従って平文コンテンツ 1 8 の利用ができるように構成することにより、特別なサーバ装置等を設けることなく特定の利用者のみが平文コンテンツ 1 8 に基づく W e b コンテンツの閲覧ないし利用を行うことができる。

【 0 0 4 4 】

例えば、利用者 A に対応する利用制限情報 A にブラウザ 1 2 の印刷機能のみを許可する利用制限規則が登録されていれば、表示部 8 のブラウザ画面上にはブラウザ 1 2 の印刷機能の利用を促すブラウザ補助機能 2 0 が生成され、利用者 A は当該印刷機能によりブラウザ画面上に生成された平文コンテンツ 1 8 の印刷を行うことができる。また、利用者 B に対応する利用制限情報 B にブラウザ 1 2 の印刷機能及び画面コピーを許可する利用制限規則が登録されていれば、表示部 8 のブラウザ画面上にはブラウザ 1 2 の印刷機能及び画面コピーの利用を促すブラウザ補助機能 2 0 が表示され、利用者 B は当該印刷機能及び画面コピー機能によりブラウザ画面上に表示された平文コンテンツ 1 8 の印刷、画面コピーを行うこと

ができる。

【 0 0 4 5 】

なお、利用制限情報 1 9 に登録する利用制限規則としては、ブラウザ画面に表示されたイメージデータの印刷許可する印刷許可、保存を許可する保存許可、画面コピーを許可各する画面コピー許可等がある。また、印刷許可、保存許可等の回数、さらにはイメージデータを再生して閲覧することができる閲覧回数及び閲覧期間等についても利用制限規則として登録することができる。

【 0 0 4 6 】

次に、コンテンツ再生装置 3 の利用制限処理について図 4 を用いて詳細に説明する。利用制限処理とは、ブラウザ 1 2 の判別、起動状態を監視する処理を行う一方、コンテンツ再生制御プログラム 1 0 の起動により使用禁止となったブラウザ 1 2 のコンテンツ利用機能を暗号化データ 1 0 に含まれた利用制限情報 1 9 に基づいて利用者に許可する処理である。起動しているブラウザ 1 2 の種類とバージョンはキー制御ライブラリ 1 5 によって判別する (S 0 1) 。コンテンツ再生制御プログラム 1 0 が許可していないブラウザである判断した場合は、復号化の処理を中断する指示をコンテンツ再生制御プログラム 1 0 に与えてその後の復号化に関する処理を行わずに終了する (S 0 2 , S 0 3) 。

【 0 0 4 7 】

ブラウザ 1 2 の起動状態の監視はキー制御ライブラリ 1 5 に起動されたインスタンス管理ライブラリ 1 6 により行う (S 0 4) 。ブラウザ 1 2 が終了していると判断した場合は、インスタンス管理ライブラリ 1 6 からキー制御ライブラリ 1 5 に対してその後の処理を終了する指示が与えられ、キー制御ライブラリ 1 5 はコンテンツ再生制御プログラム 1 0 の起動により使用禁止としたブラウザ 1 2 に対するキー制御を開放する (S 0 5 , S 0 6) 。

【 0 0 4 8 】

インスタンス管理ライブラリ 1 6 がブラウザ 1 2 が起動していると判断した場合は、キー制御ライブラリ 1 5 はブラウザ機能制限処理を継続し、端末装置 3 に接続されたキーボード等の入力手段 (図示省略する。) からのイベントをハンドリングする (S 0 7) 。具体的には、入力手段から印刷実行、画面コピー等のキ

ー入力がされた場合に（S 0 8）、そのキー入力を利用者毎に設定されたコンテンツ利用制限情報 1 9 を考慮して管理対象、すなわち使用許可されていない操作であるか否かを判断し（S 0 9）、管理対象であると判断した場合はそのキー入力を無効化する（S 1 0）。

【 0 0 4 9 】

以上の処理はブラウザ 1 2 の起動が終了するまで継続され、その間における入力手段からのキー入力が暗号化データ 1 0 から読み出された利用制限情報 1 9 に基づいて利用制限される。

【 0 0 5 0 】

図 6 はコンテンツ再生制御プログラム 9 の起動により表示部 8 のブラウザ画面上に生成されたコンテンツ再生制御プログラム 9 のインタフェース画面等を示す表示画面図である。図 6 において、2 2 はコンテンツ再生制御プログラム 9 により無効化されたブラウザ 1 2 の表示メニュー（コンテンツ利用機能）、2 3 はブラウザ補助機能 2 0 内に生成された印刷機能である。通常、ブラウザ画面に表示された Web コンテンツの内容はブラウザ 1 2 の表示メニューを操作して印刷、保存等することが可能であるが、無効化された表示メニュー 2 2 に対するマウス、キーボードによる操作はキー制御ライブラリ 1 5 の無効化処理により一切受け付けられないので、端末装置 3 の利用者はこの無効化された表示メニュー 2 2 を通しての印刷や保存等の操作を行うことはできない。しかし、識別情報の一致した利用者は暗号化データ 1 0 から復元された利用制限情報 1 9 に基づいてブラウザ画面上にブラウザ補助機能 2 0 が生成されるので、このブラウザ補助機能 2 0 を介して許可された機能、例えば印刷機能 2 3 等を操作してブラウザ画面上に表示された Web コンテンツの印刷、保存、画面コピー等を行うことができる。

【 0 0 5 1 】

以上のように、実施の形態 1 による端末装置 3 においては、Web コンテンツを表示するブラウザ 1 2 のコンテンツ利用機能がコンテンツ再生制御プログラム 9 によって使用禁止にされる一方、このコンテンツ利用機能に代わるブラウザ補助機能 2 0 を生成して特定の利用者のみがブラウザ画面上に表示された Web コンテンツを利用できるようにしたので、第三者による不正利用を確実に防止する

ことができる。また、ブラウザ補助機能 2 0 は利用者毎に登録した利用制限情報 1 9 に従って生成されるので、各利用者は識別情報の一致した利用制限情報 1 9 により許可されたブラウザ補助機能 2 0 しか利用することができず、コンテンツの利用が許可された利用者による不正利用をも防止することができ、ブラウザ画面上に表示された W e b コンテンツの漏洩を確実に防止することができる。

【 0 0 5 2 】

また、復号化ライブラリ 1 の復号化処理により復元された平文コンテンツ 1 8 及び利用制限情報 1 9 はすべてコンテンツ再生制御プログラム格納部 6、すなわち端末装置 3 内に設けられた R A M 等のメモリ上のみで管理されるので、W e b コンテンツが表示された後はこれら平文コンテンツ 1 8 及び利用制限情報 1 9 が端末装置 3 内のハードディスクやキャッシュ等に残らず、この点においても W e b コンテンツの漏洩を確実に防止することができる。

【 0 0 5 3 】

また、コンテンツ再生制御プログラム 9 は、W e b ブラウザと連携して起動する機械依存のないプログラムであり、ブラウザ 1 2 上で当該プログラムを実行することができるので、一般に公開されている各種の W e b ブラウザと連携して使用することができる。これにより、一般に公開されているブラウザと異なる新規なブラウザを作成する必要がない。

【 0 0 5 4 】

なお、以上の説明では利用者の認証に関し、あらかじめ利用者に通知されてあるユーザ I D、パスワードを使用するものについて説明したが、別途配布する共通鍵を併用するようにしてもよい。このように共通鍵を併用することで、たとえユーザ I D、パスワードが漏洩しても共通鍵が一致しなければ上述したような閲覧を行うことは不可能であり、サーバ装置 1 から配信されるコンテンツの利用者をより厳密に特定することができる。

【 0 0 5 5 】

実施の形態 2.

次に、この発明の実施の形態 2 について図 7 及び図 8 を用いて説明する。図 7 は実施の形態 2 によるコンテンツ再生方法を実現するためのシステム概要図、図

2は図1に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。図7及び図8において、24はCD-ROM、DVD等の記録媒体、25はCD-ROMドライブ、DVD-ROMドライブ等の媒体読取装置であり、実施の形態2によるコンテンツ再生システムでは、暗号化データ10を保存する手段がネットワーク2に接続されたサーバ装置1ではなく、CD-ROM、DVD等の記録媒体24である。

【0056】

従って、コンテンツ再生装置3bは記録媒体24からコンテンツ再生制御プログラム9及び暗号化データ10を取得する必要がある、図7及び図8に示すように記憶媒体23内に保存されたデータを端末装置3内に読み出すためのCD-ROMドライブ、DVD-ROMドライブ等の媒体読取装置25が内蔵もしくは外付けされている。なお、図中、同一符号は同一または相当部分を示し、これらについての詳細な説明は省略する。また、実施の形態2における端末装置3においても図6に示すようなブラウザ画面等が表示される。

【0057】

実施の形態2においても、利用者が暗号化データ10を復号化して閲覧する場合は、まずブラウザ12を起動し、ブラウザ画面上に生成された呼び出し用HTML部11によりコンテンツ再生制御プログラム9の転送要求を行う。但し、実施の形態2によるコンテンツ再生装置3bにおいては、呼び出し用HTML部11の呼び出し用HTMLは記憶媒体24が挿入された媒体読取装置25を示している。そして、この呼び出し用HTML部11にアクセスすることにより記録媒体24に保存されたコンテンツ再生制御プログラム9への転送要求が実行され、記録媒体24に保存されたコンテンツ再生制御プログラム媒体読取装置25を介して端末装置3内のコンテンツ再生制御プログラム格納部6に格納される。なお、以下の動作については実施の形態1とほぼ同様であり説明を省略する。

【0058】

以上のように、実施の形態2によるコンテンツ再生装置3bにおいても、Webコンテンツを表示するブラウザ12のコンテンツ利用機能がコンテンツ再生制御プログラム9によって使用禁止にされる一方、このコンテンツ利用機能に代わ

るブラウザ補助機能 2 0 を生成して特定の利用者のみがブラウザ画面上に表示された W e b コンテンツを利用できるようにしたので、第三者による不正利用を確実に防止することができる。また、ブラウザ補助機能 2 0 は利用者毎に登録した利用制限情報 1 9 に従って生成されるので、各利用者は識別情報の一致した利用制限情報 1 9 により許可されたブラウザ補助機能 2 0 しか利用することができず、コンテンツの利用が許可された利用者による不正利用をも防止することができ、ブラウザ画面上に表示された W e b コンテンツの漏洩を確実に防止することができる。

【 0 0 5 9 】

また、復号化ライブラリ 1 7 の復号化処理により復元された平文コンテンツ 1 8 及び利用制限情報 1 9 はすべてコンテンツ再生制御プログラム格納部 6、すなわち端末装置 3 b 内に設けられた R A M 等のメモリ上のみで管理されるので、これら平文コンテンツ 1 8 及び利用制限情報 1 9 が端末装置 3 b 内のハードディスクやキャッシュ等に残らず、ブラウザ 1 2 の操作によるデジタルコンテンツの漏洩を確実に防止することができる。

【 0 0 6 0 】

【発明の効果】

この発明は、以上説明したように構成されているので、ブラウザ備えている各種のコンテンツ利用機能の使用が半強制的に制限される一方、識別情報の一致した特定の利用者は利用制限情報に基づいてブラウザ画面上に表示された W e b コンテンツの印刷、保存、画面コピー等を行うことができ、第三者による不正利用を確実に防止することができる。また、各利用者は識別情報の一致した利用制限情報 1 9 により許可されたブラウザ補助機能 2 0 しか利用することができず、コンテンツの利用が許可された利用者による不正利用をも防止することができ、ブラウザ画面上に表示された W e b コンテンツの漏洩を確実に防止することができる。これにより、特別のサーバ装置を設けることなく、簡易に情報漏洩の防止を実現することができる。なお、オンラインもしくはオフラインのいずれによって配信されるデジタルコンテンツについても適用することができる。

【 0 0 6 1 】

また、コンテンツ再生制御プログラムは、サーバ装置 1 又は記憶媒体 2 3 に保存されたコンテンツを閲覧するためのプログラムであるブラウザと連携して起動する機械依存のないプログラムであり、専用のブラウザを新規に作成する必要がなく、既存のブラウザをそのまま使用できる。

【図面の簡単な説明】

【図 1】 実施の形態 1 によるコンテンツ再生方法を実現するためのシステム構成図である。

【図 2】 図 1 に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。

【図 3】 コンテンツ再生装置 3 に配信される暗号化データのデータ構成を示すデータ構成図である。

【図 4】 図 1 に示すコンテンツ再生装置 3 の一連の処理について説明するためのフローチャート図である。

【図 5】 図 1 に示すコンテンツ再生装置 3 の利用制限処理について説明するためのフローチャート図である。

【図 6】 表示部 8 のブラウザ画面上に生成されたコンテンツ再生制御プログラム 9 のインタフェース画面等を示す表示画面図である。

【図 7】 実施の形態 2 によるコンテンツ再生方法を実現するためのシステム構成図である。

【図 8】 図 1 に示すコンテンツ再生装置等の具体的構成を示す機能ブロック図である。

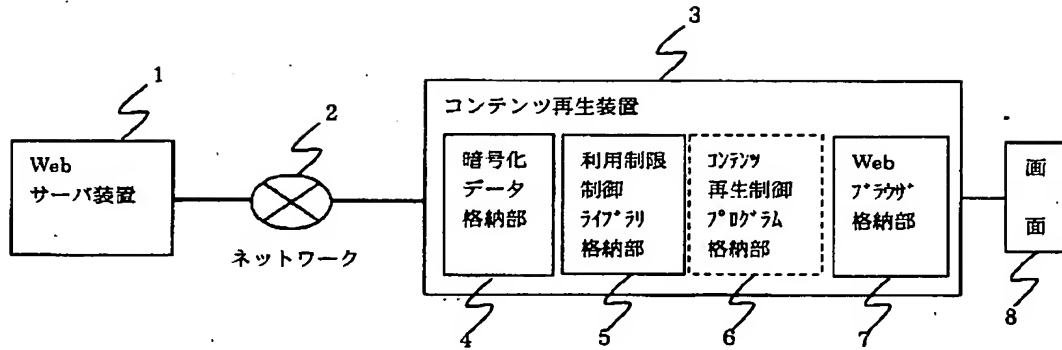
【符号の説明】

- 1 Webサーバ装置、 2 ネットワーク、 3, 3 b コンテンツ再生装置、
- 4 暗号化データ格納部、 5 利用制限制御ライブラリ格納部、
- 6 コンテンツ再生制御プログラム格納部、 7 Webブラウザ格納部、
- 8 表示部、 9 コンテンツ再生制御プログラム、 10 暗号化データ、
- 11 呼び出し用HTML部、 12 Webブラウザ、
- 13 ライブラリ制御部、 14 認証部、 15 キー制御ライブラリ、
- 16 インスタンス管理ライブラリ、 17 復号化ライブラリ、

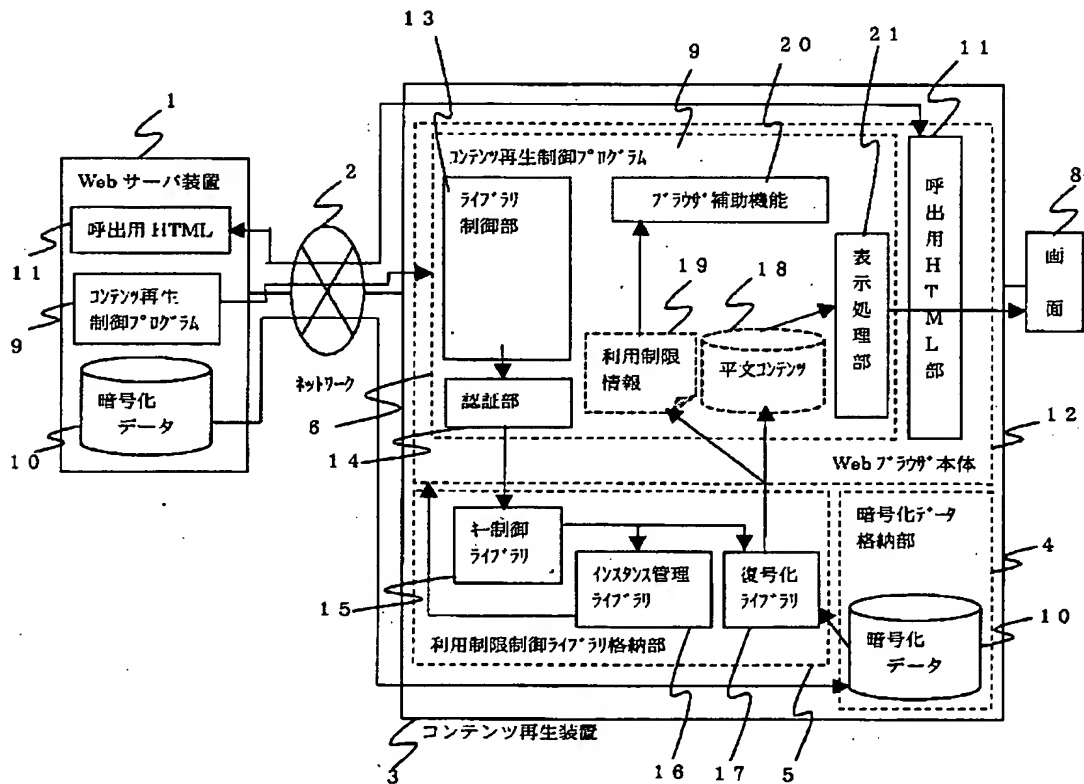
1 8 平文のコンテンツデータ、 1 9 利用制限情報、
2 0, 2 3 ブラウザ補助機能、 2 1 表示処理部、
2 2 無効化されたブラウザの表示メニュー、
2 4 記録媒体、 2 5 媒体読取装置。

【書類名】 図面

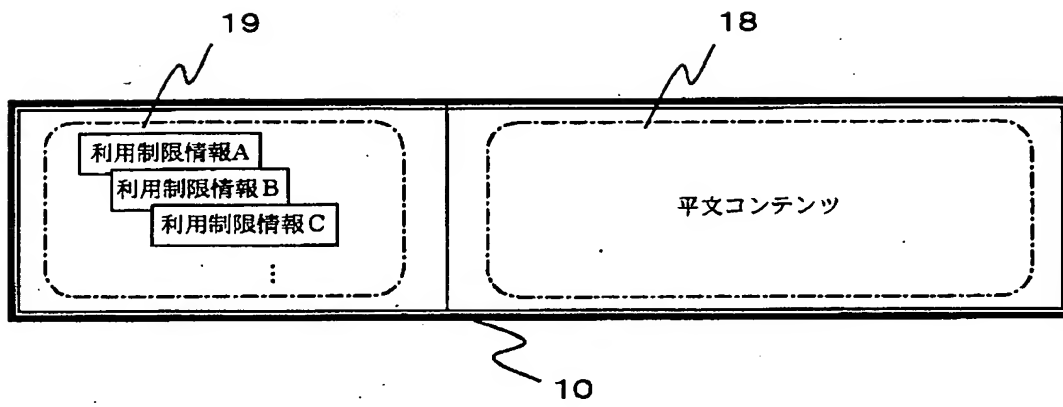
【図 1】



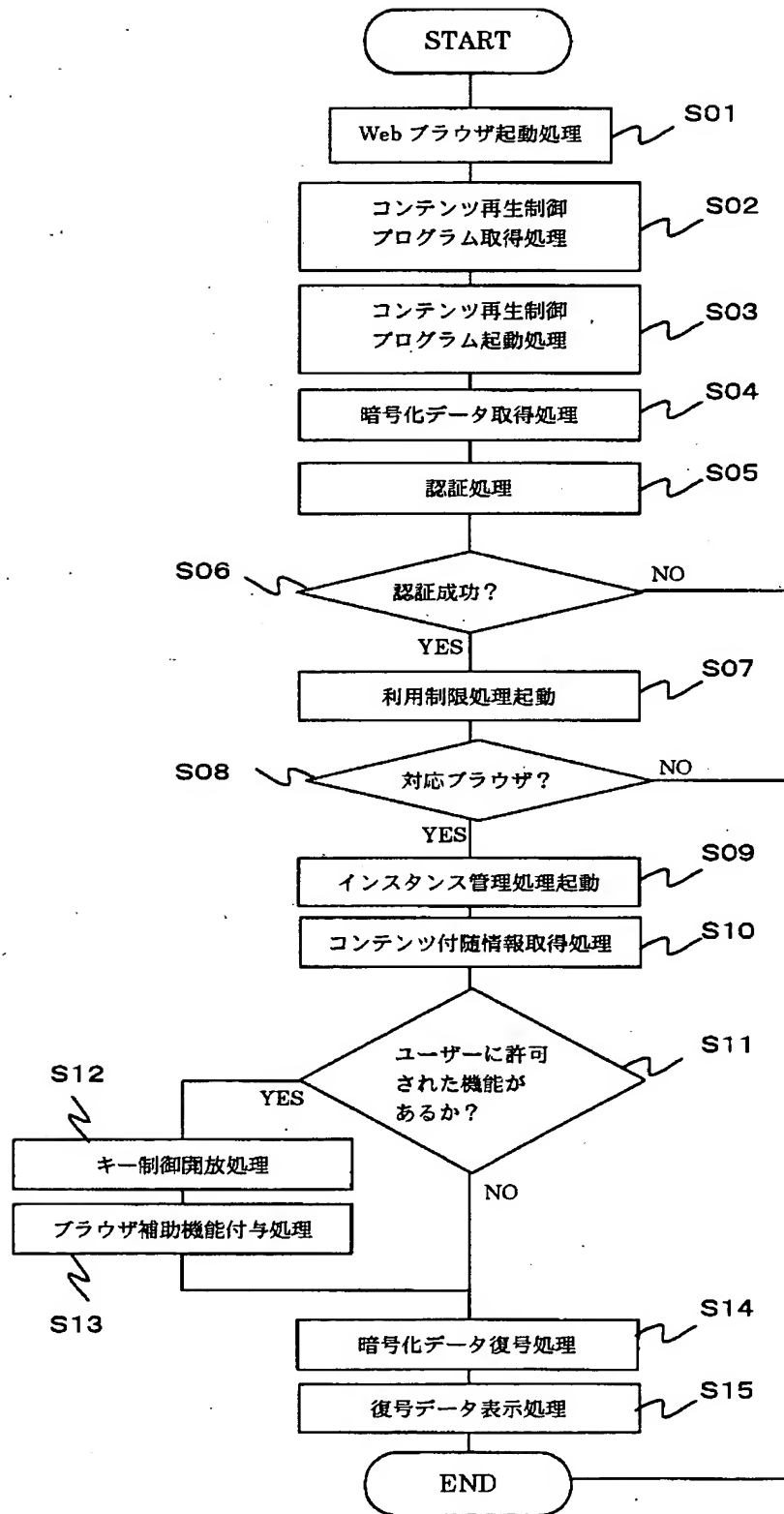
【図 2】



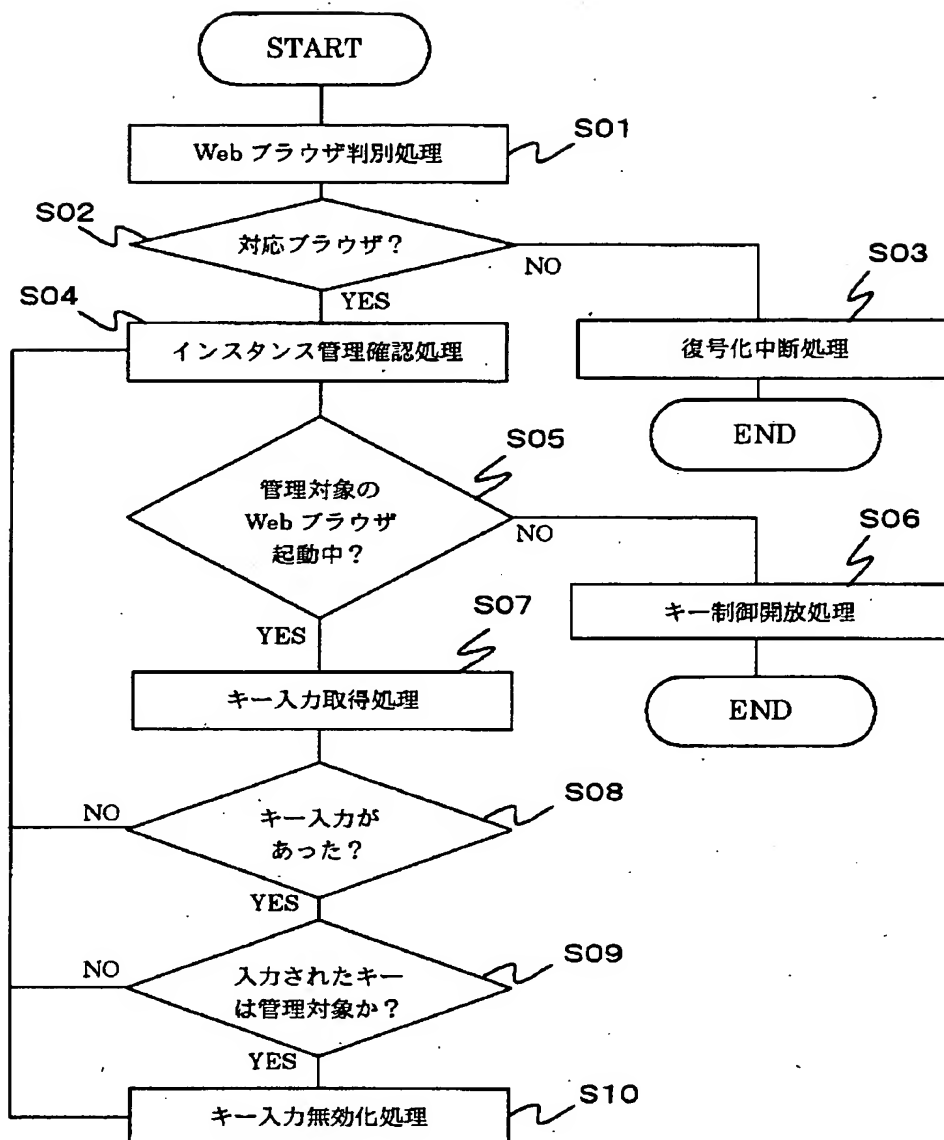
【図 3】



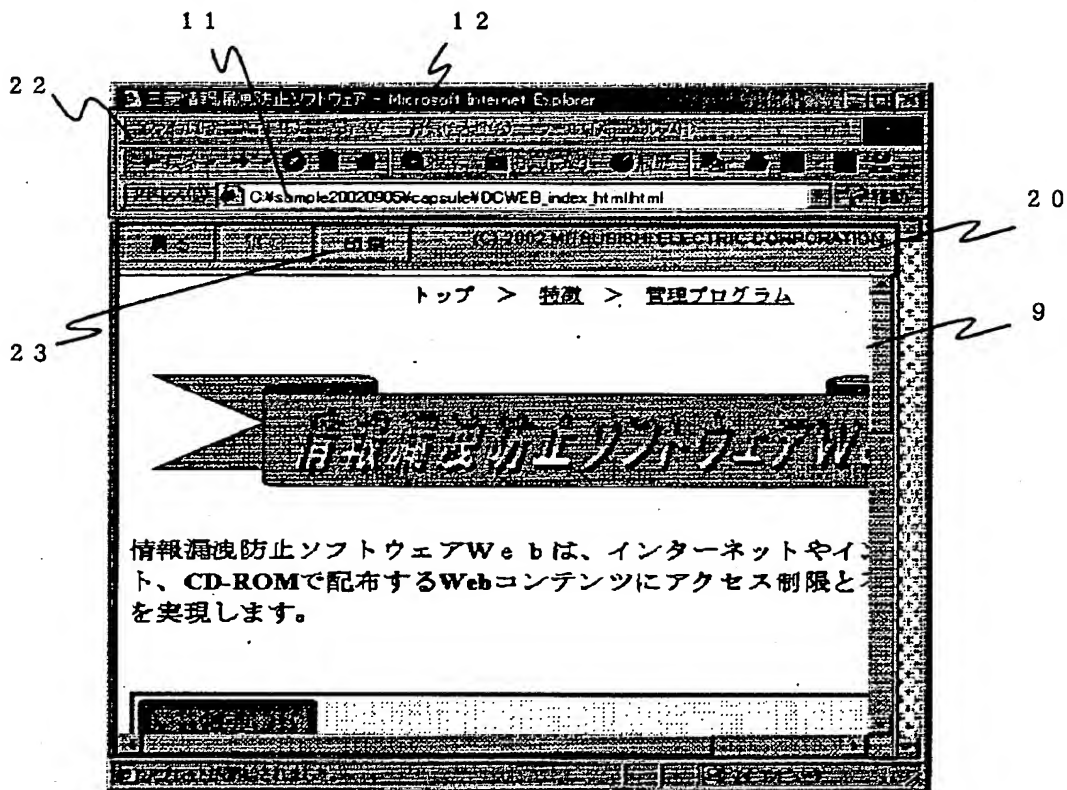
【図 4】



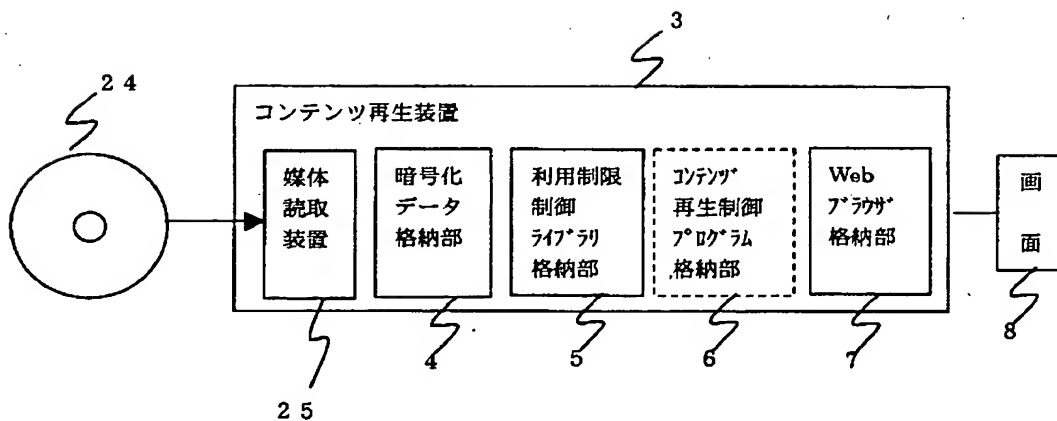
【図 5】



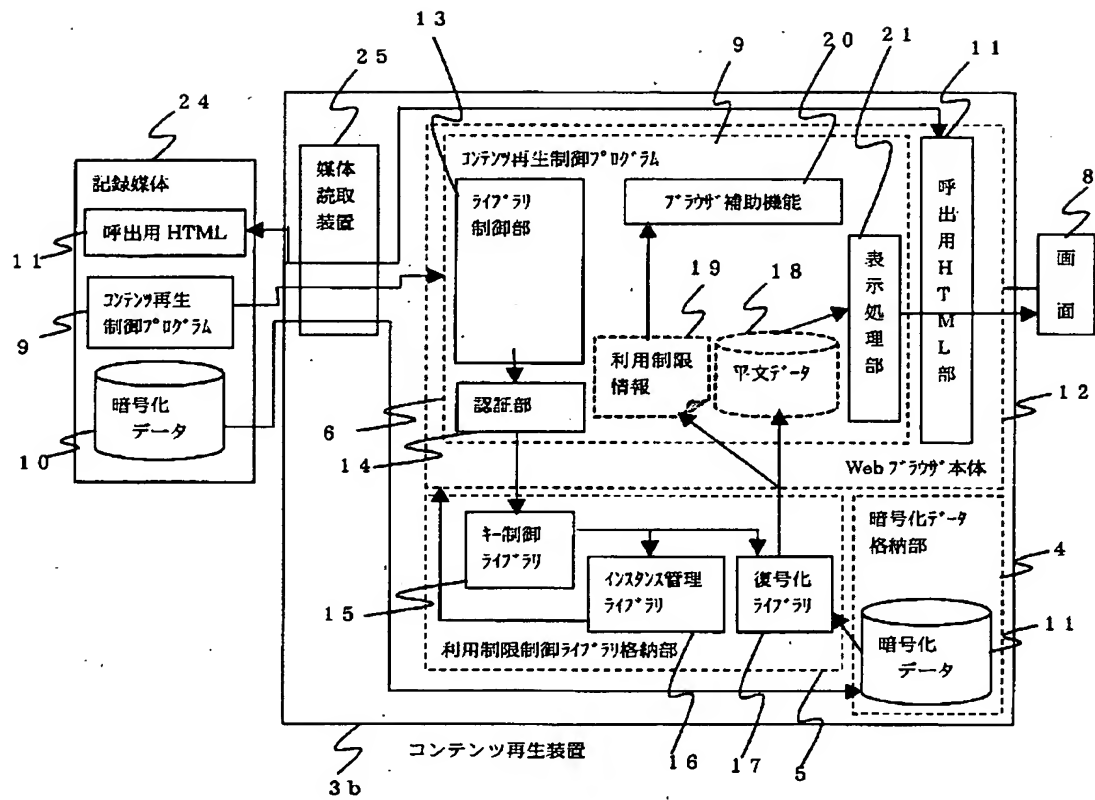
【図 6】



【図 7】



【図 8】



【書類名】 要約書

【要約】

【課題】 特別のサーバ装置等を設けることなく、コンテンツ再生装置において表示したコンテンツの不正利用ないし第三者への情報漏洩を防止する。

【解決手段】 暗号化データを取得し、この暗号化データから復元したコンテンツデータによりイメージデータを再生してブラウザのブラウザ画面上に表示させるコンテンツ再生装置において、前記暗号化データを復号化処理する復号化手段と、この復号化手段により復元されたコンテンツデータ及びその利用制限情報を一時的に記憶する記憶手段と、この記憶手段に記憶された前記コンテンツデータにより再生したイメージデータを前記ブラウザ画面上に表示する表示処理手段と、前記ブラウザのコンテンツ利用機能を使用禁止にする一方、前記コンテンツデータの利用制限情報に応じたブラウザ補助機能を生成し、このブラウザ補助機能により前記使用禁止になったコンテンツ利用機能を実行するコンテンツ再生制御手段とを備えた。

【選択図】 図 2

出 願 人 履 歴 情 報

識別番号 [000006013]

1. 変更年月日	1990年 8月24日
[変更理由]	新規登録
住 所	東京都千代田区丸の内2丁目2番3号
氏 名	三菱電機株式会社